Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:
Monday 4 January 2021 – Friday 22 January 2021

Supervised hours: 4 hours | Paper Reference **20158K**

Information Technology

Unit 11: Cyber Security and Incident Management

Part B

You must have:
Forensic_Analysis.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set tasks of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 4-hour, **Part B** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- **Part A** materials must not be accessed during the completion of **Part B**.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this Part is 37.

Turn over ▶

W67700A

1/1/1

W 6 7 7 0 0 A

Pearson

Instructions to Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of 3 weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 4-hour **Part B** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

An electronic template for activity 4 is available on the website for centres to download for learner use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Invigilators may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part B** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

Each learner will need to submit 2 PDF documents, within their folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 26th January 2021.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your invigilator may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. The folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

You will need to submit 2 PDF documents, within your folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work in to your invigilator.

Set Task Brief

Caelcabben Manor Estate

Caelcabben Manor Estate (CME) occupies a valley in southern England. CME has been owned by the Caelcabben family since the manor house was built in the 1300s. The current owner is Andrew Caelcabben.

Like many other historic homes, the manor house and estate are run as a tourist attraction. The manor house contains the estate office and an apartment where Andrew lives.

Andrew has many years of experience in estate management but considers himself an IT user rather than an IT specialist. He uses CME's administrative staff for most computing tasks.

The CME staff include a Technical Manager, Joanne Reedsman, and two electricians. They look after all electrical items on the estate, including the IT system. Joanne has completed a basic training course in system administration. She intends to take further courses this year. The electricians have completed a network maintenance course.

Figure 1 show the area around the manor house.

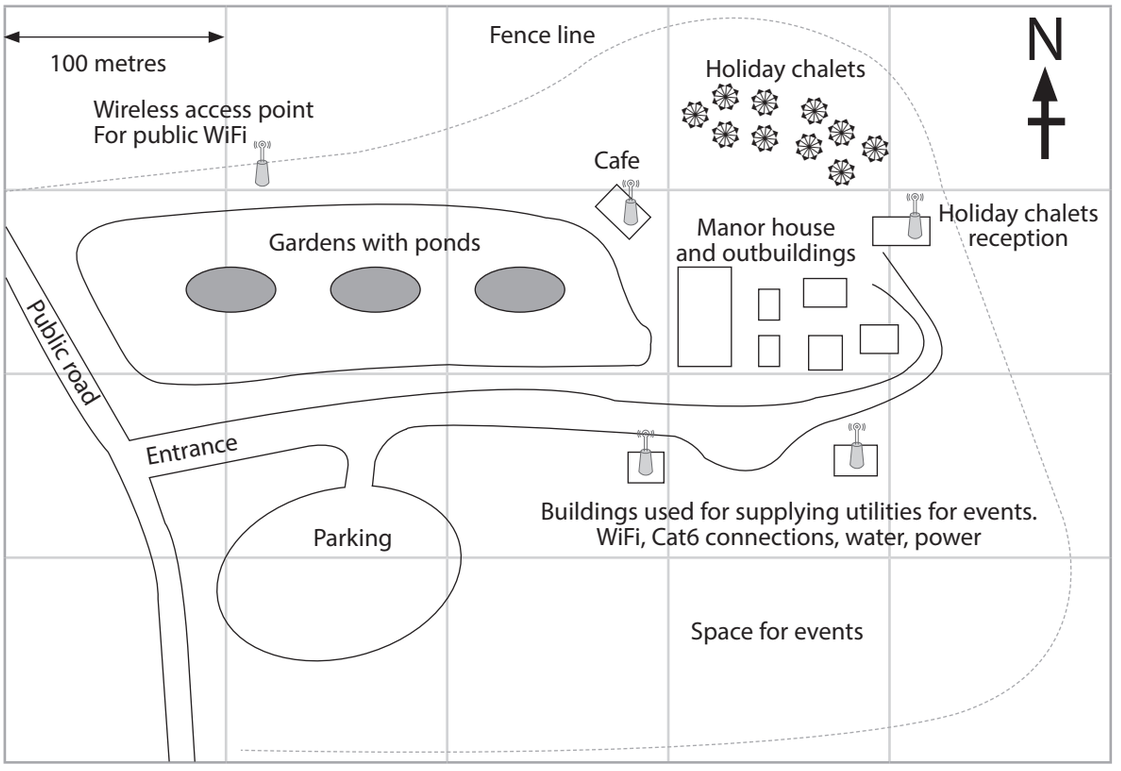


Figure 1

Client brief

You advised Andrew and Joanne on cyber security matters when the CME network was improved and extended. Now, a few months later, Andrew has asked you to review the investigation of a cyber security incident.

The incident occurred during the first weekend in January this year.

On the Monday morning, one of the staff, Chelsi Geongran, went to see Joanne about something that had happened over the weekend.

Chelsi had received a threatening email while at work the previous day and was very upset about what it said. Joanne was concerned about the content of the email, but also about the security implications of Chelsi having received it at work.

Joanne told Andrew about the incident and was asked to carry out an investigation.

Evidence items from the security incident at Caelcabben Manor Estate

Evidence items include:

1. Technical Manager's report
2. Email
3. Email filter rules
4. Network diagram
5. Report on system integrity
6. Cyber security document – incident management policy.

1. Technical Manager's report

Mon. 4th Jan. 2021. 10:00

Joanne Reedsman

Technical Manager, Caelcabben Manor Estate

Cyber security incident report. Incident Number 20210101

Situation

The estate had guests in the chalets for the Xmas and New Year holidays, so we had staff on 24/7 from Sun 20th Dec to Sun 3rd Jan. I had the weekend of the 2nd – 3rd Jan off, leaving a rota of our admin assistants running the estate office and the chalet reception. Andrew was at home and on call for emergencies.

Chelsi Geongran is our guest liaison assistant and was in charge of the chalet reception team. She should have been off on the Monday but came in to the estate office first thing in the morning and asked to talk to me privately. She seemed very upset and I made time for her straight away.

Interview with Chelsi

The interview took place from 0915 to 0930 on Monday 4th Jan 2021. It was recorded as is standard practice for all personnel interviews.

The interview transcript is summarised as numbered bullet points to make things clearer. The original transcript is in Chelsi's file and has been marked as confidential.
Chelsi has signed this section of the report to indicate that she accepts it as a fair summary of the interview.

1. Chelsi was in the estate office on the Sunday (3rd Jan) afternoon when she received an email **(see evidence item 2)**.
2. She has no idea who 'watch43672' is and has never used or heard of temporarymail.com
3. She agrees that shopCG is one of her passwords and says that it is only used for retail sites where she has to create an account to place an order.
4. One of Chelsi's roles in CME is to source items and make purchases where our main suppliers do not have suitable goods.
5. She uses the CME credit card to make purchases for CME. She does not tick the box to have the card details stored on any sites except those of our main suppliers.
6. She made several purchases before Xmas in preparation for the holidays. These were all confirmed by email and the goods have arrived.
7. Chelsi admits to doing a 'bit of Christmas shopping' for herself as well and was worried about losing her job. She used her own credit card for these purchases and the goods have arrived.
8. I assured Chelsi that her job was safe and advised her to use a password manager in future. This would allow her to use a different password for every site and make it easier to see where a compromised password might have been obtained.
9. I added to the email filter rules **(see evidence item 3)**, to prevent a repeat of the incident.

Post interview

I didn't think it likely that there would be any follow up from the email but thought it best to tell Andrew about it just in case some video was sent to him.

He then told me that he had received an identical email, this time from watch43859@temporarymail.com. He had ignored it as the password given was an old one that he had not used in over a year and he wasn't worried about losing his job. I added the new address to the filter.

Andrew was concerned that there may have been some truth in the emails and that Chelsi's password could have been found by a keylogger. He asked me to look at the possibility of a system intrusion. I prepared a second report on actions taken in checking the system **(see evidence item 5)**.

Conclusions

I believe that the email was a fishing expedition and that it is unlikely to be followed up by any further action.

I think that the system remains secure but there is a possibility that some aspects of the email may be true **(see evidence item 5)**, and I have concerns about how the passwords and email addresses were obtained.

2. Email

To: Chelsi<Chelsi.Geongran@Caelcabben_Estate.com>

From: Watcher <watch43672@temporarymail.com>

Date: 3/1/2021, 13:55

Subject: Your webcam

I am aware shopCG is your passphrases. Lets get directly to point. No person has paid me to check about you. You don't know me and you are probably thinking why you are getting this mail?

actually, i installed a software on a shopping web-site and do you know what, you visited this web site. When you were viewing, your browser started out operating as a Remote control Desktop that has a keylogger which provided me with access to your screen as well as webcam. Just after that, my software gathered your complete contacts from your social networks, as well as Outlook addreses and then i made a double video. First part displays the screens you were viewing and next part displays the recording of your web camera, yea it is you. and yea it shows you shopping when yu should be working.

You actually have two different possibilities. We should read up on the choices in aspects:

1st option is to neglect this email. as a consequence, i most certainly will send out your video recording to every bit of your contacts that has your work address and then just think concerning how you keep your job.

Number two option is to compensate me. You'll make the payment by Bitcoin (if you do not know this, search for 'how to buy bitcoin' in search engine) the price is 0.1 Bitcoin We will refer to it as a donation. Then, i most certainly will instantaneously erase your video footage. You could continue your daily life like this never took place and you will never hear back again from me.

Bitcoin address to send to: 16f5c3TjkUosquTE6q7wes2EVNgbCy26RS

[CaSe SeNSiTiVe copy and paste it]

if you may be curious about going to the authorities, look, this mail can not be traced back to me. I have taken care of my actions. i am just not trying to ask you for very much, i just like to be paid. if i don't receive the Bitcoin, i will send your video to all of your work contacts that probably means your boss. Nonetheless, if i receive the payment, i'll erase the recording immediately. If you need evidence, reply with Yes! and i will send out your video to immediately. This is the nonnegotiable offer thus don't waste mine time & yours by replying to this email message.

3. Email filter rules

Examples of rules for the email filter on the CME mail server.

- The basic Virus Rule set is provided by the email software and receives regular updates. New rules may be added manually.
- The software has a heuristics function that flags possible spam. If the user confirms that the email is spam, the software writes a Spam Pattern Rule to identify similar spam in the future.
- Users may add email addresses to Blacklist Rules.

Example Virus Rules

```
# Subject:  Your **** photos attached
header      Subject=~ /your (lost|stolen|friend's|secret) (photo|photos) attached/i
describe    Subject is common virus/trojan sign
score       3.0

body  LOCKY|CRYPTOWALL_Type_TEST1    /I am sending copies of the documents as attachments/i
body  LOCKY|CRYPTOWALL_Type_TEST2    /Thank you very much for your reply/i
body  LOCKY|CRYPTOWALL_Type_TEST3    /I have attached the financial report you requested./i
body  LOCKY|CRYPTOWALL_Type_TEST4    /I am sending you the invoice you requested/i
body  LOCKY|CRYPTOWALL_Type_TEST5    /Attached please find the documents you requested/i
body  LOCKY|CRYPTOWALL_Type_TEST6    /wrong data file you received from me/i
body  LOCKY|CRYPTOWALL_Type_TEST7    /attached is concerned with the company database/i

# Subject:  ATTN: Invoice-[random code]
header      Subject =~ /Attention Invoice KF-2144437990/i
describe    Subject is common virus/trojan sign
score       3.5

body  MACRO_VIRUS_type_TEST1         /I am sending a copy of the invoice as an attachment/i
body  MACRO_VIRUS_type_TEST2         /attached invoice (Microsoft Word Document) (/i
body  MACRO_VIRUS_type_TEST3         /I have attached the (Microsoft Word Document) invoice/i
```

Example Spam Pattern Rules

```
body        YOUR_WEBCAM / I am aware **** is your passphrases/
describe    YOUR_WEBCAM 'Your webcam' match
score       4.0

body        WE_ARE_NOT_SPAM / We are not spammer./
describe    WE_ARE_NOT_SPAM 'We are not spam' match
score       3.0

body        BRING_EMAIL1 /We can bring you more business and find new clients by
            our email services/
describe    BRING_EMAIL1 Bring business by email match
score       2.0

body        KNOWN_PHONENUM_SPAM1 /877-228-1545/
describe    KNOWN_PHONENUM_SPAM1 Known spam phone number - 877-228-1545
score       4.0
```

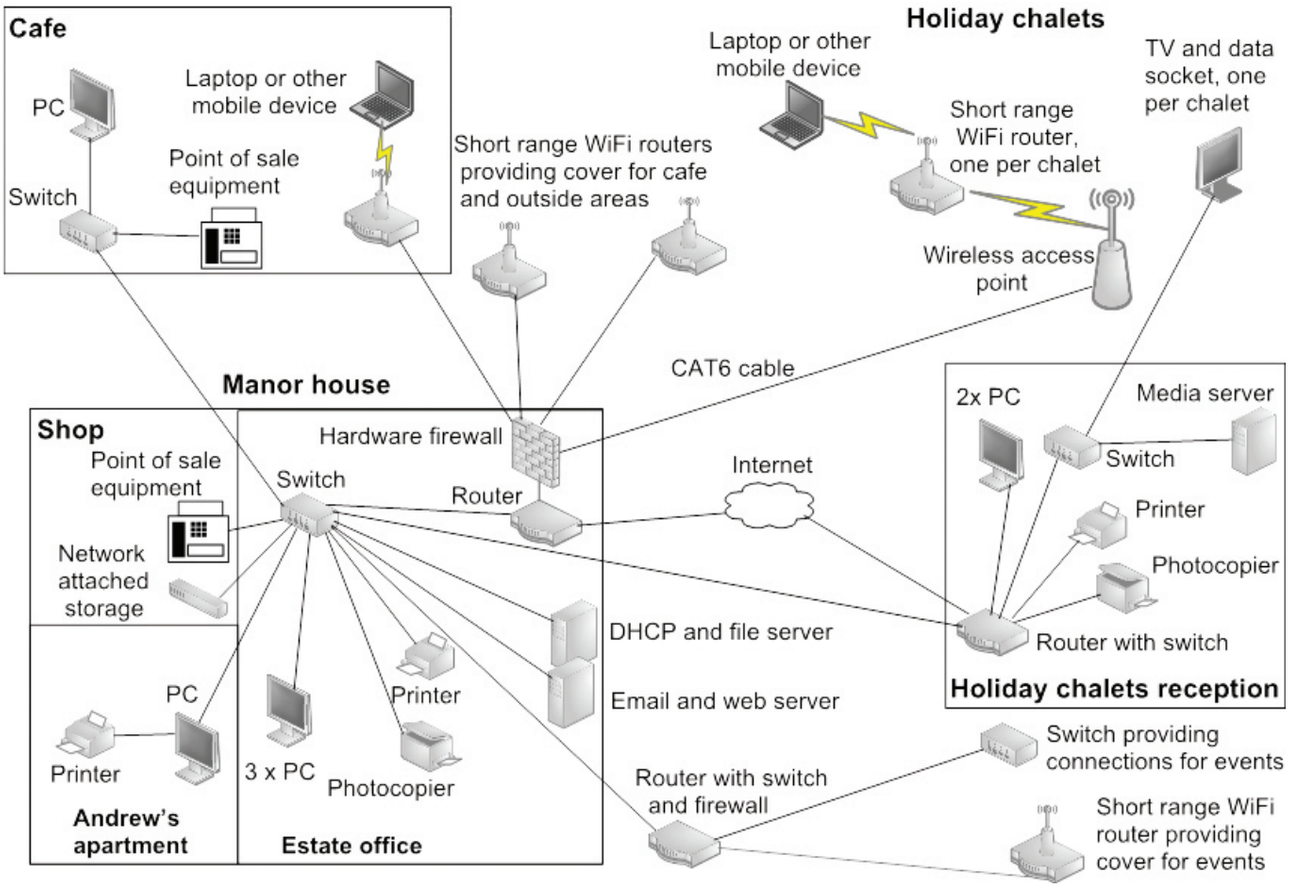
Example Blacklist Rules

```
# Known addresses of people who have tried to extort CME staff
blacklist_from watch43672@temporarymail.com
blacklist_from watch43859@temporarymail.com

# Known addresses of person XXXX who has been abusive to CME staff
blacklist_from thpusenet@yahoo.ca
blacklist_from *@darkshadows.ca
blacklist_from viewstalkers@yahoo.ca

# Known addresses of persons sending mailworms
blacklist_from waamoudr@anonymbox.com
blacklist_from johnsmith7896897@gmail.com
blacklist_from joeblow57@googlemail.com
blacklist_from bendspamrules@hotmail.com
```

4. Network diagram



5. Report on system integrity

Wed. 6th Jan. 2021. 15:00

Joanne Reedsman

Technical Manager, Caelcabben Manor Estate

Actions taken to check system integrity following the cyber security incident

Malware scans

The new system is based on Linux but there are some Windows laptops being used. The servers are storing documents in Windows/Microsoft formats.

All Windows machines were scanned with the latest version of CME's anti-virus software. No problems were found.

All stored files were scanned with Linux-based anti-virus software. No problems were found.

Webcam use

I was able to use Process Explorer on the Windows laptops to check what had been using the webcams. Unfortunately most uses were linked to browsers and Host Processes. There was no way of telling what they were being used for.

The Linux machines do not have a built-in webcam. The one we use for video calls is only plugged in when needed.

Physical intrusion

I checked the Staff WiFi access logs for the last month. There were numerous unknown devices trying to connect. This is normal as members of the public often try to get onto the network. Only staff devices were found to have connected.

I asked the electricians to check the WAPs and switches in public areas. They are protected by locked plastic boxes and the electricians reported that there was no sign of forced entry.

Logs

Printouts of the WiFi and Process Explorer logs, plus the anti-virus report, were stored in the hard copy folder for this incident.

Conclusions

I believe that the system has not suffered a security breach but there remains a possibility that the webcams on Windows laptops may have been used as described in the email.

6. Cyber security document – incident management policy

Incident management team

The team leader is Joanne Reedsman, Technical Manager.

The team leader shall co-opt other team members as needed.

Incident reporting

Any member of staff who considers that an IT-related security incident has occurred must report it as soon as possible to the Computer Security Incident Response Team (CSIRT) leader.

Initially it may be reported verbally but this must be followed up by an email. It is the responsibility of the CSIRT to maintain detailed documentation on the incident from first report to final resolution.

Security incidents may include:

- theft of IT equipment
- theft of company data
- unauthorised access to CME IT systems
- infection of CME IT systems with malware.

Incident response procedures

(a) Theft of IT equipment

- Theft of IT equipment is a very serious issue. Any thefts must be reported at once to the CSIRT leader, initially a verbal report must be made followed up by email, providing as much information as possible (location and type of equipment, when it was last seen, etc.).
- The CSIRT leader must ascertain if the item has actually been stolen (or if it is just missing).
- If the item is confirmed as stolen, the CSIRT leader must inform the police and contact the finance department so they can inform insurers.
- The CSIRT leader must prepare a report on the theft to Andrew Caelcabben and if needed justify the finances required to replace the stolen item.

(b) Theft of CME data

- Theft or loss of CME data may occur in a number of different ways. Any loss of data must be reported at once to the CSIRT leader, initially a verbal report must be made followed up by email.
- The CSIRT must investigate the loss and identify exactly what data has been lost or stolen and when the incident occurred.
- Where it is suspected that customers' personally identifiable information has been accessed a report must be made to Andrew Caelcabben.
- Having identified what has been lost or stolen and how, the CSIRT can retrieve backups and restore the data as soon as possible.
- The CSIRT should review the incident and implement procedures to prevent future losses.

(c) Infection of CME IT systems with malware

- Any member of staff who suspects that any CME IT system has been infected with malware must report it at once to the CSIRT leader, initially a verbal report must be made, followed up by email.
- The infected system should be shut down as soon as possible.
- The CSIRT will investigate the infection and take appropriate measures to resolve the infection and restore the system.

(d) Unauthorised access to CME systems

- Any member of staff who suspects that there has been unauthorised access to any CME system must report it at once to the CSIRT leader, providing as much detail as possible (which system, how access was obtained). Initially a verbal report must be made, followed up by email.
- The CSIRT will thoroughly investigate the incident and identify how the unauthorised access was obtained.
- The CSIRT will take whatever action is required to prevent future occurrences (e.g. change passwords).

Part B Set Task

You must complete ALL activities within the set task.

Produce your documents using a computer.

Save your documents in your folder ready for submission using the formats and naming conventions indicated.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

You have been advising Andrew Caelcabben on cyber security. Now he has asked you to review the investigation of a cyber security incident.

Activity 4: Forensic incident analysis

Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident at Caelcabben Manor Estate.

Consider possible causes of the incident and come to a conclusion about the most likely cause of the incident.

Refer to evidence items 1–5 inclusive.

Produce a forensic incident analysis using the template **Forensic_Analysis.rtf**

Save your completed forensic incident analysis as a PDF in your folder for submission as **activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 4 = 14 marks)

Activity 5: Security report

Review the incident. Suggest improvements and explain how they would prevent a similar incident in the future.

Areas for improvement are:

- adherence to forensic procedures
- the forensic procedure and current security protection measures
- the security documentation.

Read the set task brief and evidence items 1–6 inclusive when answering the question.

Save your completed security report as a PDF in your folder for submission as **activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 5 = 20 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART B = 3 MARKS
TOTAL FOR PART B = 37 MARKS